CLOUDFLARE

LÖSUNGSLEITFADEN

Coffee Shop-Networking

Modernisierung des Netzwerks an jedem beliebigen Standort mit SASE für minimale Hardware-Ausstattung und unkomplizierte Vernetzung bei einheitlicher Sicherheit

Jeder Standort wird wie ein Café behandelt

Von einem Café aus zu arbeiten ist einfach: Latte bestellen, Laptop aufklappen und sich über WLAN mit den benötigten Anwendungen verbinden. Moderne Unternehmen lassen sich davon inspirieren, um an verschiedenen Standorten – etwa Zweigstellen, Geschäften, Restaurants oder Produktionsstätten – eine flexiblere und günstigere Netzwerkarchitektur zu implementieren.

Dieses „Coffee Shop-Networking"-Modell verspricht die nahtlose Konnektivität, die Mitarbeitende heute erwarten, ohne die Komplexität eines herkömmlichen nichtöffentlichen Netzwerks.

Grundlage für diese Anpassung bildet die agile SASE-Plattform **Cloudflare One**. Durch die Umstellung von einem Mosaik aus verschiedenen Konnektivitäts- und Sicherheits-Appliances auf ein von Grund auf einheitliches Cloud-Netzwerk können Sie:

- **Kosten und lokale Präsenz auf ein Mindestmaß verringern** nach dem Prinzip „Light Branch, Heavy Cloud".
- **Überall das gleiche Nutzererlebnis bieten**: ob zu Hause, im Büro oder im Café.
- **Zero Trust-Sicherheit durchsetzen** mit hochpräzisen Richtlinien, die nicht vom Netzwerkstandort, sondern von der Identität bestimmt werden.

Cloudflare macht den Unterschied

- **Einheitliche WAN- und Zero Trust-Sicherheitsdienste** wurden für das Zusammenspiel auf einer einzigen SASE-Plattform entwickelt. Damit gehören komplizierte, von Sicherheitsfunktionen losgelöste SD-WAN-Overlay-Konfigurationen der Vergangenheit an.
- **Globale Skalierbarkeit und Konsistenz** dank einer dreimal größeren Zahl von Netzwerkstandorten als andere SASE-Anbieter.
- **Modulare und flexible Zugangswege** zur Unterstützung von „Any-to-Any"-Vernetzung für L1–L7 mit einer einzigen Steuerungsebene. Schluss mit dem umständlichen Navigieren durch separate SD-WAN- und Sicherheitsarchitekturen.
- **Niemals für Nutzerbandbreite zahlen.** Bei Cloudflare fließt Nutzer-Traffic nicht in die WAN-Kosten ein: Ihnen werden keine Bandbreitenkosten zusätzlich zu den Nutzerlizenzen in Rechnung gestellt.

Empfohlene Vorgehensweise

SCHRITT 1
Anwendungszugriff für Nutzer modernisieren

VPN ersetzen
durch ZTNA von Cloudflare

SCHRITT 2
Anbindung von Zweigstellen vereinfachen

Standorte verbinden
mit Cloudflare WAN

SCHRITT 3
Web- und Cloud-Zugang schützen

Internet-Breakout absichern
mit dem SWG von Cloudflare

LAUFEND

Hardware reduzieren

UX vereinfachen

Sicherheit skalieren

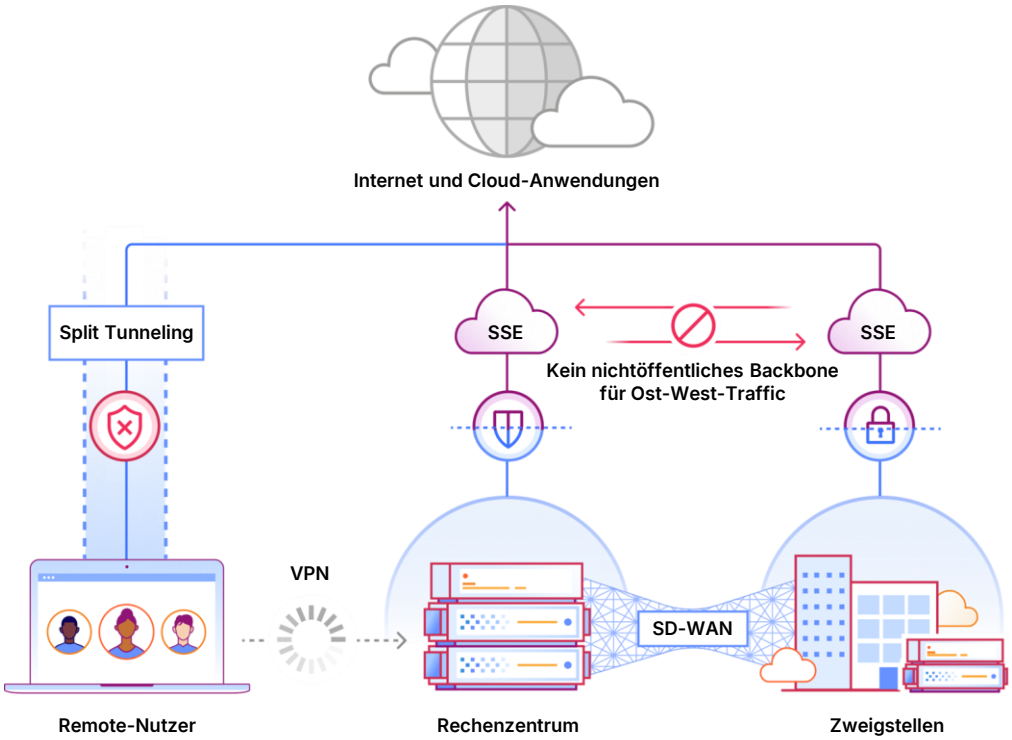
Coffee Shop-Networking einführen

SASE-Konsolidierung fortsetzen

Die Herausforderung: Unzusammenhängende SD-WAN-Produkte und an bestimmte Dienste gekettete SSE-Lösungen

SD-WAN hat in den 2010er Jahren durch die Kombination von Internet und MPLS für eine Kostensenkung gesorgt. Das Verfahren war jedoch zur Vernetzung von Gebäuden gedacht, nicht von Menschen. Das hat oft folgende Konsequenzen:

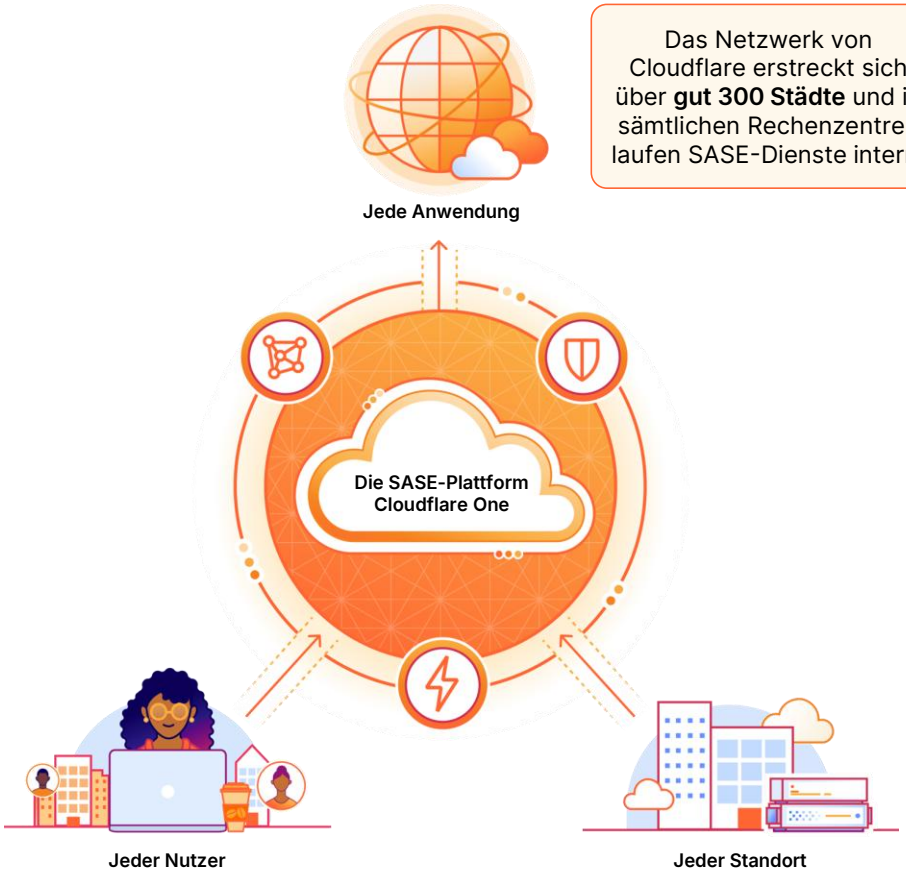
- **Großer Verwaltungsaufwand und hohe Kosten:** Overlay-Konfigurationen sind zu komplex und Teams zahlen doppelt: für Nutzer-Sicherheitslizenzen und standortbasierte Bandbreite.
- **Schlechte Performance:** Remote-Mitarbeitende hängen weiterhin von langsamen VPN ab.
- **Fragmentierte Sicherheit:** Viele Anbieter erwerben und verknüpfen gesonderte SD-WAN- und SSE-Dienste, was eine uneinheitliche Richtliniendurchsetzung mit sich bringt.



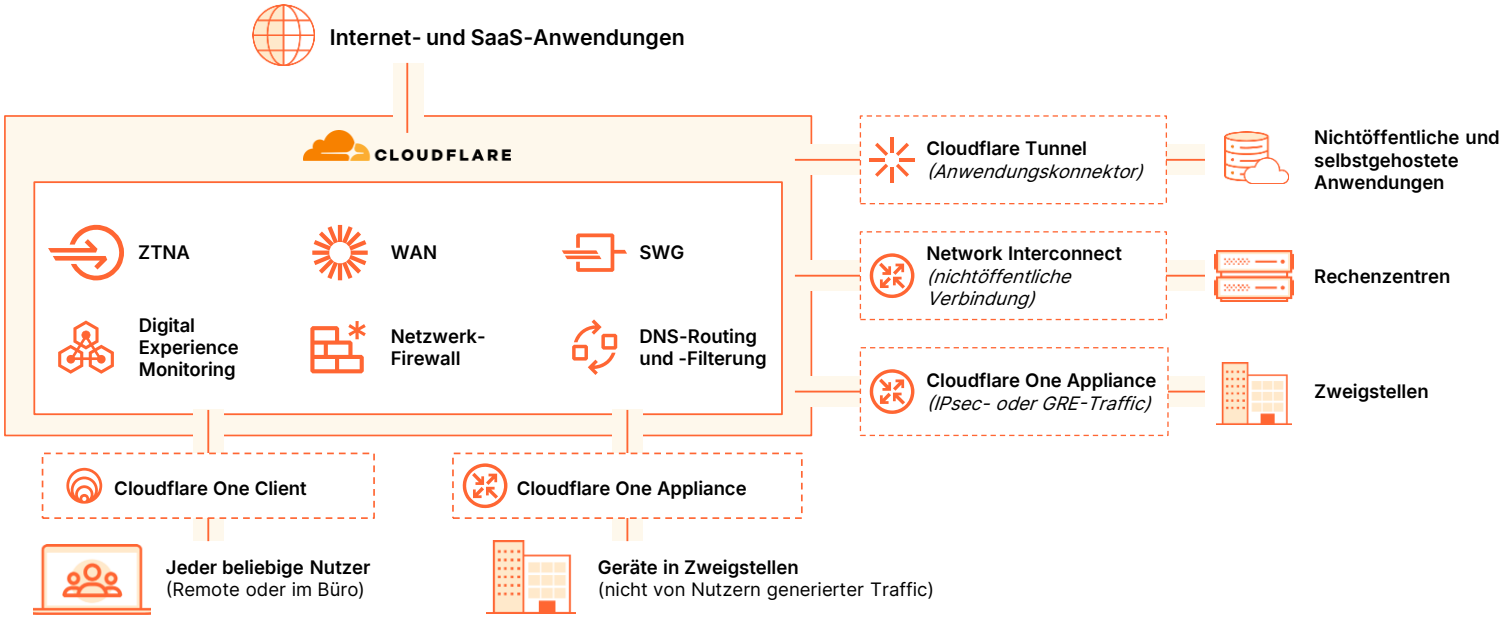
Die Lösung: Die wahrhaft einheitliche SASE-Architektur von Cloudflare

Cloudflare One führt Netzwerk- und Sicherheitsdienste auf einer gemeinsamen Steuerungsebene zusammen. Das hat unter anderem folgende Vorteile:

- **Keine Dienstverkettung mehr:** Jeder Service ist an jedem Standort mit einer Single-Pass-Überprüfung verfügbar, um einheitliche Skalierbarkeit zu gewährleisten.
- **Optimierte Konnektivität:** Ost-West-Traffic durchläuft das nichtöffentliche Backbone des Cloudflare-Netzwerks per KI-gesteuertem, automatischem Routing über unsere Rechenzentren, um Probleme im Internet zu vermeiden und nicht vollständig auf Peering-Netzwerke angewiesen zu sein.
- **Modulare Architektur:** Alle Dienste sind interoperabel, sodass die Steuerungselemente jeweils im eigenen Tempo und in beliebiger Reihenfolge aufgesetzt werden können. Das gleiche gilt für Zugangswege wie unseren Geräte-Client, Appliances und physische Interconnections. So bewahren Sie sich bei der Entscheidung darüber, wie der Traffic zu Cloudflare geleitet wird, Ihre Flexibilität.



So funktioniert's



Schritt 1: Anwendungszugriff für Nutzer modernisieren

Mit dem Ersatz von VPN durch Cloudflare Access können webbasierte, im SaaS-Modell bereitgestellte und nichtöffentliche Anwendungen abgesichert werden. Dieser ZTNA (Zero Trust Network Access)-Dienst setzt identitätsbasierte Regeln für jede Anwendung individuell durch. Zu den Zugangswegen und weiteren Funktionen für diesen Schritt gehören:

- Cloudflare One Client: Dieser kann für umfassende Proxy-Steuerung und quantensichere Verbindungen auf allen Geräten implementiert werden.
- Cloudflare Tunnel: Damit lassen sich Anwendungen oder nichtöffentliche Subnetze ohne VM-Infrastruktur mit Cloudflare verbinden.
- Cloudflare Digital Experience Monitoring: Die Lösung ermöglicht eine proaktive Fehlerbehebung und löst Performance-Probleme von Geräten, Netzwerken und Anwendungen.

Cloudflare empfiehlt, den Nutzerzugriff auf Anwendungen allein über ZTNA und den Geräte-Client zu steuern, um einheitliche Bedingungen für den Zugriff sowohl aus der Ferne als auch von Firmenstandorten aus zu gewährleisten.

Schritt 2: Konnektivität für Geräte in Zweigstellen vereinfachen

Die Anbindung von Geräten, die sich nicht wie ein Mensch authentifizieren können (z. B. Drucker, Kameras, WLAN-Zugangspunkte, IoT- und OT-Geräte), wird geschützt.

Cloudflare WAN steuert den Traffic der verschiedenen Standorte – ohne die Komplexität herkömmlicher Hardware oder SD-WAN-Overlays. Zu den Zugangswegen und weiteren Funktionen gehören:

- Cloudflare One Appliance: Der Traffic wird mit dieser schlanken, über die Cloud verwalteten Hardware- oder virtuellen Appliance über sichere IPsec-Tunnel geleitet.
- Cloudflare Network Interconnect: Die Rechenzentrumsinfrastruktur wird direkt über eigens dafür vorgesehene physische oder virtuelle Verbindungen mit Cloudflare vernetzt.
- Cloudflare Network Firewall: L3/L4-Traffic wird gefiltert und es kann ein System zur Erkennung von Eindringlingen aktiviert werden.

Mit den Schritten 1 und 2 werden die Abhängigkeit von lokalen Appliances und der Personalbedarf vor Ort gesenkt.

Schritt 3: Internet-Breakout absichern

Der an das öffentliche Internet und SaaS-Anwendungen geleitete Traffic wird mit Cloudflare Gateway geschützt. Dieses Secure Web Gateway (SWG) filtert und analysiert den für das Web bestimmten Datenverkehr mithilfe von DNS, HTTP und Netzwerkrichtlinien. Auch andere SASE-Funktionen stehen überall und jederzeit zur Verfügung:

- **Absicherung von Daten:** Es können weitere SASE-Kontrollmechanismen wie der Schutz vor Datenverlust (Data Loss Prevention – DLP), Browserisolierung und ein extern agierender Cloud Access Security Broker (CASB) zugeschaltet werden.
- **DNS-Routing und -Filterung:** Cloudflare bietet als Anbieter rekursiver und autoritativer DNS-Auflösung einzigartige Vorteile.
- Zum Beispiel können DNS-Einträge für interne Ressourcen in einem nichtöffentlichen Netzwerk verwaltet und dann DNS-Richtlinien zur Auflösung der Abfragen von nichtöffentlichen und selbst gehosteten Ressourcen festgelegt werden.

Damit verlagert sich die Gewährleistung der Sicherheit von lokal betriebenen Firewalls auf die SASE-Plattform.

Erfolgsgeschichten von Kunden

US-Einzelhandelskette
[Mehr erfahren]

Einfachere, automatisierungsfreundliche Lösung zur Verwaltung der Netzwerkkonnektivität für **über 250 Filialen** durch kleine IT-Abteilung

Französisches Forschungsinstitut

Verringerung der Abhängigkeit von VPN und MPLS-Verbindungen für **gut 50 Zweigstellen** und Forscher weltweit

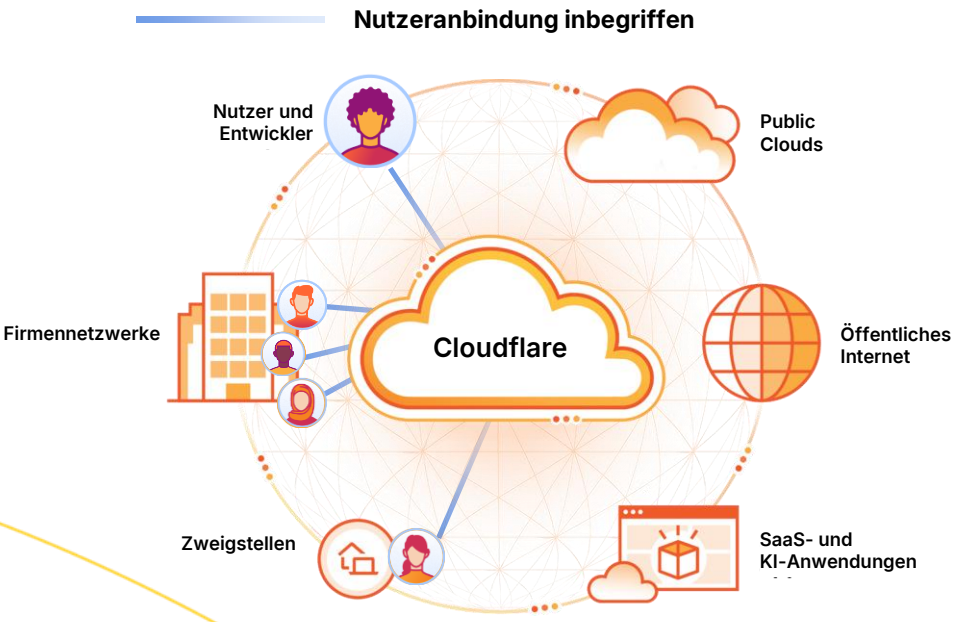
Ticketverkauf und Entertainment

Ausweitung der Konnektivität für **über 250 Standorte** von Australien auf neue Weltregionen

Global tätiger Produzent

SASE-Konsolidierung bei einem einzigen Anbieter zur Eindämmung des Technologie-Wildwuchses, einschließlich mehrerer VPN in über **70 Ländern**

Einfaches Preismodell für SASE



Niemals für Nutzerbandbreite zahlen

Sie zahlen jeweils nur die Lizenz für die Anbindung Ihrer Remote-, Hybrid- und Zweigstellen-Nutzer. Für Geräte, auf denen unser User-Agent installiert ist, werden Ihnen niemals Bandbreitenkosten in Rechnung gestellt.

Mit jeder Lizenz wird Ihr WAN erweitert

Ersetzen Sie teure WAN-Verträge. Jede Nutzerlizenz trägt zu einem gemeinsamen Bandbreitenpool bei, der Ihr gesamtes Netzwerk von Büros und Rechenzentren verbindet.

 +49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/